IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Cain Application No.: 09/661,273 Filed: 9/13/2000 Title: System, Device & Method for Receiver Access Control in an Internet Television System Attorney Docket No.: 120-194	Group Art Unit: 2453 Examiner: Nguyen

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Sir:

Please enter this Reply Brief in response to the Examiner's Answer of June 1, 2009.

I. Real Party in Interest

The real party in interest is Nortel Networks Limited.

II. Related Appeals and Interferences

Appellants are not aware of any related appeals or interferences.

III. Status of the Claims

This is an appeal from an office action dated December 1, 2008, in which claims 1-55 are subject to final rejection. Claims 1-55 are currently pending in the present application. No claims have been allowed. Claims 2-14, 16-24, 26-34, 36-44, and 46-54 are original. Claims 1, 15, 25, 35, 45, and 55 are previously presented. The rejections of claims 1, 15, 25, 35, 45 and 55 are the subject of this appeal.

IV. Status of Amendments

All submitted amendments have been entered and considered.

V. Summary of Claimed Subject Matter

The claimed subject matter concerns access control in an Internet television system. For many years, television signals were almost exclusively delivered via land-based wireless broadcast. The television signals were not encrypted, and anyone with a receiver could view the channel being broadcast. Subscription-based cable and satellite television service has now displaced

broadcast television in some regions, although many of the broadcast television channels are still provided over cable and satellite. Cable and satellite systems often require use of a subscriber set-top box to decode and decrypt the incoming television signal. One purpose of the set-top box is to prevent unauthorized viewing of the channels, i.e., by non-subscribers. More recently, the Internet is being considered for delivery of television signals. One proposal for delivering television over the Internet is to use Internet Protocol ("IP") multicasting. In particular, a television channel could be carried by a multicast group, i.e., a unique multicast group would exist for each channel. In order to change channels, the television or set-top box would migrate to a different multicast group. However, it is technically challenging to both exclude non-subscribers from particular multicast groups and permit the speedy channel changes to which subscribers have become accustomed, i.e., to have security and fast group membership changes.

The independent claims are supported by the specification and drawing as indicated below in bold.

1. (previously presented) An access control method for an internet television system where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel, the access control method comprising:

distributing multicast group access control information from a distribution device to a plurality of access devices for use by the access

devices in authenticating subsequent requests by individual host devices to join a television channel multicast group in order to reduce delay in authentication when a host device changes television channels,

The access control information is distributed from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server. The access devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control 20 information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14-21.

wherein each access device is logically closer to the host device from which the access device receives the request than the distribution device;

FIG. 1 shows an exemplary communication system 100. The communication system 100 includes a distribution server 110 in communication with an access device 130 such as a router or switch over a network 120. A host device 140 accesses the network 120 via the access device 130. Page 5, lines 26-29.

receiving, by one of the access devices, a subsequent request by one of the host devices to join the television channel multicast group in order to change television channels;

When the host interface logic 408 receives a request from the host device 140 to join a television channel multicast group, the access control logic 406 retrieves access control information from the database 404 and uses the access control information to determine whether the host device 140 is authorized to join the television channel multicast group. Page 9, line 30 through page 10, line 3.

determining, by the access device, whether the host device is authorized to join the television channel multicast group, and receive a particular television channel, based upon the access control information distributed from the distribution device; and

When the host interface logic 408 receives a request from the host device 140 to join a television channel multicast group, the access control logic 406 retrieves access control information from the database 404 and uses the access control information to determine whether the host device 140 is authorized to join the television channel multicast group. Id. If the host device 140 is authorized to join the television channel multicast group, then the 5 access control logic 406 admits the host device 140 to the television channel multicast group. Page 10, lines 3 through 6.

admitting, by the access device, the host device to the television channel multicast group if and only if the host device is determined to be authorized to join the television channel multicast group,

If the host device 140 is authorized to join the television channel multicast group, then the 5 access control logic 406 admits the host device 140 to the television channel multicast group. Id. If the host device 140 is not authorized to join the television channel multicast group, then the access control logic 406 rejects the host device 140. Page 10, lines 9 through 11.

whereby the access device receives the access control information before it is needed for determining whether the host device is authorized to join the multicast group, thereby facilitating changing channels by reducing authentication delay.

The access control information is distributed from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server. The access devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14 through 21.

15. (previously presented) An apparatus for distributing access control information in an internet television system where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the apparatus comprising:

maintenance logic and memory operably coupled to maintain multicast group access control information; and

The distribution server 110 maintains the access control information in a database. The distribution server 110 may obtain the access control information in various ways. Page 6, lines 26-27.

distribution logic and an interface operably coupled to distribute the access control information to at least one access device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels,

In order to efficiently distribute the access control information to the access devices, the access control information is typically distributed to the access devices using a "push" mechanism by which current access control information is sent to the access devices without the access devices having to request or retrieve the access control information. The access control information may be sent by the main server at various times. For example, the access control information may be sent by the distribution server 110 periodically and/or as changes occur. The access control information typically includes a sequence number or other

identifier for identifying a specific version of access control information, and is used for differentiating between different versions of access control information. Thus, the distribution server 110 and the access device 130 implement a "push" mechanism by which the access control information is distributed from the distribution server 110 to the access device 130. Among other things, the "push" mechanism may employ unicast, multicast, or broadcast techniques. Page 7, lines 4-17.

wherein the access device is operable to transmit the channel to the host device and is logically closer to the host device than the apparatus for distributing access control information,

FIG. 1 shows an exemplary communication system 100. The communication system 100 includes a distribution server 110 in communication with an access device 130 such as a router or switch over a network 120. A host device 140 accesses the network 120 via the access device 130. Page 5, lines 26-29.

whereby the access device receives the access control information before it is needed for determining whether a host device is authorized to join a multicast group, and receive a particular television channel, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

The access control information is distributed from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting

or otherwise retrieving the access control information from the main server. The access devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14 through 21.

25. (previously presented) A computer program embedded in a tangible storage medium for controlling a computer system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the computer program comprising:

maintenance logic programmed to maintain multicast group access control information; and

The distribution server 110 maintains the access control information in a database. The distribution server 110 may obtain the access control information in various ways. Page 6, lines 26-27.

distribution logic programmed to distribute the access control information to at least one access device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels,

In order to efficiently distribute the access control information to the access devices, the access control information is typically distributed to the access devices using a "push" mechanism by which current access control information is sent to the access devices without the access devices having to request or retrieve the access control information. The access control information may be sent by the main server at various times. For example, the access control information may be sent by the distribution server 110 periodically and/or as changes occur. The access control information typically includes a sequence number or other identifier for identifying a specific version of access control information, and is used for differentiating between different versions of access control information. Thus, the distribution server 110 and the access device 130 implement a "push" mechanism by which the access control information is distributed from the distribution server 110 to the access device 130. Among other things, the "push" mechanism may employ unicast, multicast, or broadcast techniques. Page 7, lines 4-17.

wherein the access device is operable to transmit the channel to the host device and is logically closer to the host device than the apparatus for distributing access control information,

FIG. 1 shows an exemplary communication system 100. The communication system 100 includes a distribution server 110 in communication with an access device 130 such as a router or switch over

a network 120. A host device 140 accesses the network 120 via the access device 130. Page 5, lines 26-29.

whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

The access control information is distributed from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server. The access devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14 through 21.

35. (previously presented) An apparatus for providing receiver access control in an internet television system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the apparatus comprising:

distribution logic operably coupled to receive multicast group access control information from a distribution device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels;

The access control information is distributed from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server. The access devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control 20 information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14-21.

host interface logic operably coupled to receive a request from a host device to join a television channel multicast group; and

When the host interface logic 408 receives a request from the host device 140 to join a television channel multicast group, the access control logic 406 retrieves access control information from the database 404 and uses the access control information to determine whether the host device 140 is authorized to join the television channel multicast group. Page 9, line 30 through page 10, line 3.

access control logic operably coupled to determine whether the host device is authorized to join the television channel multicast group based upon the access control information,

When the host interface logic 408 receives a request from the host device 140 to join a television channel multicast group, the access control logic 406 retrieves access control information from the database 404 and uses the access control information to determine whether the host device 140 is authorized to join the television channel multicast group. Id. If the host device 140 is authorized to join the television channel multicast group, then the 5 access control logic 406 admits the host device 140 to the television channel multicast group. Page 10, lines 3 through 6.

wherein the apparatus is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and

FIG. 1 shows an exemplary communication system 100. The communication system 100 includes a distribution server 110 in communication with an access device 130 such as a router or switch over a network 120. A host device 140 accesses the network 120 via the access device 130. Page 5, lines 26-29.

whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

The access control information is distributed from the main server to the access devices in such a way that the access devices receive

the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server. The access devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14 through 21.

45. (previously presented) A computer program embedded in a tangible storage medium for controlling a computer system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the computer program comprising:

distribution logic programmed to receive multicast group access control information from a distribution device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels;

The access control information is distributed from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server. The access

devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control 20 information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14-21.

host interface logic programmed to receive a request from a host device to join a television channel multicast group; and

When the host interface logic 408 receives a request from the host device 140 to join a television channel multicast group, the access control logic 406 retrieves access control information from the database 404 and uses the access control information to determine whether the host device 140 is authorized to join the television channel multicast group. Page 9, line 30 through page 10, line 3.

access control logic programmed to determine whether the host device is authorized to join the television channel multicast group based upon the access control information,

When the host interface logic 408 receives a request from the host device 140 to join a television channel multicast group, the access control logic 406 retrieves access control information from the database 404 and uses the access control information to determine whether the host device 140 is authorized to join the television channel multicast group. Id. If the host device 140 is authorized to join the television channel multicast

group, then the 5 access control logic 406 admits the host device 140 to the television channel multicast group. Page 10, lines 3 through 6.

wherein the host interface logic is executed by a device that is logically closer to the host device than the distribution device,

FIG. 1 shows an exemplary communication system 100. The communication system 100 includes a distribution server 110 in communication with an access device 130 such as a router or switch over a network 120. A host device 140 accesses the network 120 via the access device 130. Page 5, lines 26-29.

whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

The access control information is distributed from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server. The access devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14 through 21.

55. (previously presented) An internet television system for delivering a video signal to a host device for display, comprising:

a distribution device in communication with at least one access device over a communication network, wherein the distribution device uses a predetermined push mechanism to distribute multicast group access control information to the at least one access device in order to reduce delay in authentication when a host device changes television channels, and

In order to efficiently distribute the access control information to the access devices, the access control information is typically distributed to the access devices using a "push" mechanism by which current access control information is sent to the access devices without the access devices having to request or retrieve the access control information. The access control information may be sent by the main server at various times. For example, the access control information may be sent by the distribution server 110 periodically and/or as changes occur. The access control information typically includes a sequence number or other identifier for identifying a specific version of access control information, and is used for differentiating between different versions of access control information. Thus, the distribution server 110 and the access device 130 implement a "push" mechanism by which the access control information is distributed from the distribution server 110 to the access device 130. Among other things, the "push" mechanism may employ unicast, multicast, or broadcast techniques. Page 7, lines 4-17.

wherein the at least one access device uses the access control information to control access to at least one television channel multicast group,

When the host interface logic 408 receives a request from the host device 140 to join a television channel multicast group, the access control logic 406 retrieves access control information from the database 404 and uses the access control information to determine whether the host device 140 is authorized to join the television channel multicast group. Page 9, line 30 through page 10, line 3.

wherein the access device is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

The access control information is distributed from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server. The access devices maintain the access control information in a database for subsequent use in authenticating hosts. Because the access device obtains the access control information before the request is received from the host, there is essentially no delay in authenticating the host. This in turn reduces delays in changing channels. Page 5, lines 14 through 21.

VI. Grounds of Rejection to be Reviewed on Appeal

A. Claims 1, 15, 25, 35, 45 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable based on US 5,748,736 (Mittra) in view of US 6,621,793 (Widegren).

VII. Argument

A. Widegren does not qualify as prior art.

This application was filed on September 13, 2000. Widegren was filed on a later date, May 21, 2001. Because this application was filed before Widegren, the citation of Widegren as prior art necessarily relies upon priority documents. Widegren claims priority to two provisional applications: 60/206,186 filed May 22, 2000; and 60/246,501 filed November 6, 2000. Only the 60/206,186 provisional application has an earlier filing date than this application. In spite of Applicant's request, the Office has provided no evidence that the cited subject matter is present in the 60/206,186 provisional application. The Office cannot reasonably assume that the features for which the reference is cited are not either new matter in the utility application, or disclosed in the 60/246,501 provisional applications which fails to predate this application. Since the rejection cannot stand without Widegren, the rejection should be reversed.

The Examiner's Answer counters the point above by providing only slightly more specificity. In particular, the examiner now asserts that the features are shown in 60/206,186 somewhere at pages 9 and 13-16. Surely the examiner could be more specific and provide a copy of the provisional. Applicant's point is that if the foundation of the rejection is a provisional application then that provisional application should be subjected to the same scrutiny as the subsequent related reference. Waiting until the final stages of appeal to vaguely cite five pages from a document that hasn't even been provided to applicant is not a reasonable basis for maintaining a rejection.

B. The cited references fail to teach distributing multicast group access control information from a distribution device to a plurality of access devices for use by the access devices in authenticating subsequent requests by individual host devices to join a television channel multicast group in order to reduce delay in authentication when a host device changes television channels.

Prior to the idea of delivering television through IP multicast, which was proposed in about the year 2000, there was no need for faster authentication because multicast was used or proposed for applications such as telephone conferencing, video conferencing, and network application sharing, in which the user does not frequently change multicast group. Delivery of television via multicast creates a new problem because in order to change channels the

television or set-top box must migrate to a different multicast group, and people tend to change channels much more rapidly and frequently than they change conference calls, etc. Further, re-authentication for migrating to a different multicast group is relatively slow in comparison with the rate of channel change expected by the typical channel surfer. Still further, it is technically challenging to exclude non-subscribers from particular multicast groups and simultaneously permit the speedy channel changes to which subscribers have become accustomed, i.e., to have both security and fast group membership changes. The presently claimed invention helps solve these problems by distributing multicast group access control information from a distribution device to a plurality of access devices for use by the access devices in authenticating subsequent requests by individual host devices to join a television channel multicast group.

Three basic criteria must be met in order to establish a *prima facie* case of obviousness. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Third, the prior art references must teach or suggest all the claim limitations. (MPEP §2143) The Office has failed to meet at least the third criteria.

The Office concedes that Mittra fails to teach distributing multicast group access control information from a distribution device to a plurality of access devices for use by the access devices in authenticating subsequent requests by individual host devices to join a television channel multicast group in order to

reduce delay in authentication when a host device changes television channels as recited in the independent claims, but asserts that Widegren does so at column 11, line 33 through column 12, line 24, column 13, line 52 through column 14, line 4, and column 15, line 30 through column 16, line 58. More specifically, the Office asserts that the "policy control filtering data" is equivalent to the claimed "multicast group access control information." However, the analogy attempted by the Office is contradicted by the Widegren reference itself. As indicated in the Abstract, Widegren describes a method for filtering and gating a data flow in a QoS connection. As described at column 15, lines 56-62:

> Policy enforcement is defined in terms of a gate implemented in the GGSN. A gate is a policy enforcement function for a unidirectional flow of packets, e.g., in either the upstream or downstream direction. At a high level, *a gate includes* a *packet classifier, a resource "envelope," and an action taken when the set of packets matching the classifier exceeds the resource envelope*. (emphasis added)

With regard to the envelope, as described at column 16, lines 44-52:

> The authorized envelope defines an upper bound, or "envelope," of the *resources that are authorized* for the set of packets defined by the packet classifier. The authorized envelope can authorize more resources than are actually used. Since the authorized envelope defines IP bearer resources towards or from the external network, it is appropriate to express it in terms of IP bearer resources, such as a *peak information rate, mean information rate, and token bucket size to or from the external network*. (emphasis added)

Clearly, the "policy control filtering data" indicates resource allocation limits relative to QoS, and <u>not whether a particular subscriber is authorized to receive particular data</u>. Indeed, as indicated at column 13, line 66 through column 14, line 1, "gating" concerns what data is allowed to enter the network based on those limits. In contrast, the claimed invention concerns whether a particular host device is authorized to receive multicast data that has already entered the network. Note that for IP multicast television delivery the QoS is not generally a subscriber or channel specific issue. In other words, the data stream is either adequate to support acceptable quality television or not, regardless of the channel being viewed or which subscriber is receiving the channel.

In view of the points discussed above it will be appreciated that the passages of Widegren cited by the Office fail to support the rejection. The passage at column 11, line 33 through column 12, line 24, describes filtering and gating a data flow in a QoS connection as the subject matter of the document. Information to support those functions is pushed to the gateway support node, but neither the information nor the described functions include distributing multicast group access control information. The passage at column 13, line 52 through column 14, line 4, discusses the gate function. However, as described in the passage, gating concerns what data is allowed to enter the network based on resource allocation limits, not *where* data that has already entered the network is delivered. Finally, the passage at column 15, line 30 through column 16, line 58 describes policy enforcement. However, none of the policy enforcement functions concern *where* data is delivered.

The Examiner's Answer counters the above by arguing that Mittra, rather than Widegren, teaches distributing multicast group access control information to access devices. More particularly, the examiner asserts that Mittra teaches distributing multicast group access control information to access devices in the abstract and columns 3 and 13-14. It is respectfully suggested that the examiner has misinterpreted the cited passages, each of which describes how to improve scalability by distributing functions to trusted servers, i.e., more devices. There is no mention of moving functions closer to subscribers so that changes can be made faster, which is the point of the present invention. In other words, "more" is not equivalent to "closer," because logical distance between subscriber and device is the source of the problem. Note that "closer" is what "each access device is logically closer to the host device from which the access device receives the request than the distribution device" means.

In view of the above it will not be surprising that Mittra actually contradicts the examiner's characterization at column 7, lines 64-65, by stating that **only the Group Security Controller** (which the Office likens to the distribution device) **has information concerning group membership**. In other words, the presently claimed invention has the access device performing access control based on group membership information obtained beforehand from the distribution device, whereas Mittra teach that the GSC withholds the group membership information from the TIs. Rather than access control, Mittra relies on distribution of keys to prevent decryption of the multicast data, i.e., Mittra

provides the encrypted data to all requestors, which the claimed invention does not do.

With regard to the boilerplate assertion that applicant has attacked references individually and the new explanation of how the references are being applied, it is submitted that the previous rejections have been lacking in explanation and ambiguous. Applicant welcomes any clarification because it helps to narrow the issues. However, the statements in Mittra which contradict the examiner's characterization cited above were already pointed out in a previous response so it can hardly be suggested that applicant has ignored the Mittra reference.

For the reasons stated above, the cited combination fails to teach or suggest all of the claim limitations cited in the independent claims. The rejections should therefore be reversed.

C. The "Response to Arguments" in the Final Office Action misinterprets both Widegren and the law.

In the Response to Arguments the Examiner cites the same passages discussed above, and characterizes them as teaching "the policy control filtering data being pushed and pre-authorized before the client request by the policy server (i.e., distribution device) to gateway GPRS support node (GGSN) (i.e., access device) **for authenticating client requested**)." (emphasis added). The Examiner misinterprets the cited passages because there is no description

whatsoever of **client authentication** in the cited passages. Client authentication simply isn't part of the teaching.

The Examiner also asserts that applicant is improperly attacking references individually where the rejection is based on a combination of references, citing *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); and *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Note that the point of law is predicated on the condition that "the rejection is based on a combination of references." The following is a quote from the Final Office Action: "Mittra does not explicitly teach distributing access control information from a distribution device to a plurality of access devices for use by the access devices in authenticating a subsequent requests by individual host device and whereby the access device receives the access control information before it is needed for determining whether the host device is authorized to join the multicast group, thereby facilitating changing channels by reducing delay."[1] The Examiner goes on to assert that Widegren teaches the feature. Because the Examiner concedes that Mittra does not teach the claim limitations at issue, and bases the rejection of the limitations solely on Widegren, the rejection of that limitation is NOT based on a combination of references. Further, it would be a waste of both the Examiner's and applicant's time to argue about a reference that both already agree does not teach the limitation at issue.

[1] Final Office Action dated 12/10/2008 at page 4 (last paragraph) through page 5.

VIII. Conclusion

The rejections are improper for at least the reasons set forth above. Appellants accordingly request that the rejections be reversed and the application put forward for allowance.

Respectfully submitted,

/Holmes W. Anderson/
Holmes W. Anderson
Reg. No. 37,272
Attorney for Assignee

Date: July 27, 2009

Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton MA 01720
(978) 264-4001

Appendix A - Claims

1. (previously presented) An access control method for an internet television system where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel, the access control method comprising:

distributing multicast group access control information from a distribution device to a plurality of access devices for use by the access devices in authenticating subsequent requests by individual host devices to join a television channel multicast group in order to reduce delay in authentication when a host device changes television channels, wherein each access device is logically closer to the host device from which the access device receives the request than the distribution device;

receiving, by one of the access devices, a subsequent request by one of the host devices to join the television channel multicast group in order to change television channels;

determining, by the access device, whether the host device is authorized to join the television channel multicast group, and receive a particular television channel, based upon the access control information distributed from the distribution device; and

admitting, by the access device, the host device to the television channel multicast group if and only if the host device is determined to be authorized to join the television channel multicast group,

whereby the access device receives the access control information before it is needed for determining whether the host device is authorized to join the multicast group, thereby facilitating changing channels by reducing authentication delay.

2. (original) The access control method of claim 1, wherein distributing the access control information from the distribution device to the access device comprises:

pushing the access control information from the distribution device to the access control device using a predetermined push mechanism.

3. (original) The access control method of claim 2, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

4. (original) The access control method of claim 3, wherein pushing the access control information from the distribution device to the access control device using the predetermined push mechanism comprises:

joining a predetermined multicast group by the access device;

sending the access control information to the predetermined multicast group by the distribution device using the reliable multicast mechanism;

receiving the access control information by the access device from the multicast group using the reliable multicast mechanism.

5. (original) The access control method of claim 2, wherein the predetermined push mechanism comprises a policy service.

6. (original) The access control method of claim 5, wherein the policy service comprises a Common Open Policy Service (COPS).

7. (original) The access control method of claim 5, wherein pushing the access control information from the distribution device to the access control device using a predetermined push mechanism comprises:

sending the access control information from the distribution device to the access device in the form of policy information using the policy service.

8. (original) The access control method of claim 2, wherein the predetermined push mechanism comprises a management mechanism.

9. (original) The access control method of claim 8, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

10. (original) The access control method of claim 8, wherein the management mechanism comprises a Command Line Interface (CU).

11. (original) The access control method of claim 8, wherein pushing the access control information from the distribution device to the access control device using a predetermined push mechanism comprises:

sending the access control information from the distribution device to the access device in the form of management information using the management mechanism.

12. (original) The access control method of claim 1, wherein determining whether the host device is authorized to join the television channel multicast group comprises:

authenticating the host device based upon the access control information.

13. (original) The access control method of claim 1, wherein admitting the host device to the television channel multicast group comprises:

joining the television channel multicast group by the access device using a predetermined multicast routing protocol.

14. (original) The access control method of claim 13, wherein the predetermined multicast routing protocol comprises a Protocol Independent Multicast (PIM) multicast routing -protocol.

15. (previously presented) An apparatus for distributing access control information in an internet television system where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the apparatus comprising:

maintenance logic and memory operably coupled to maintain multicast group access control information; and

distribution logic and an interface operably coupled to distribute the access control information to at least one access device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels, wherein the access device is operable to transmit the channel

to the host device and is logically closer to the host device than the apparatus for distributing access control information,

whereby the access device receives the access control information before it is needed for determining whether a host device is authorized to join a multicast group, and receive a particular television channel, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

16. (original) The apparatus of claim 15, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

17. (original) The apparatus of claim 16, wherein the distribution logic is operably coupled to send the access control information to a predetermined multicast group using the reliable multicast mechanism.

18. (original) The apparatus of claim 15, wherein the predetermined push mechanism comprises a policy service.

19. (original) The apparatus of claim 18, wherein the policy service comprises a Common Open Policy Service (COPS).

20. (original) The apparatus of claim 18, wherein the distribution logic is operably coupled to send the access control information to the access device in the form of policy information using the policy service.

21. (original) The apparatus of claim 15, wherein the predetermined push mechanism comprises a management mechanism.

22. (original) The apparatus of claim 21, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

23. (original) The apparatus of claim 21, wherein the management mechanism comprises a Command Line Interface (CLI).

24. (original) The apparatus of claim 21, wherein the distribution logic is operably coupled to send the access control information from the distribution device to the access device in the form of management information using the management mechanism.

25. (previously presented) A computer program embedded in a tangible storage medium for controlling a computer system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the computer program comprising:

maintenance logic programmed to maintain multicast group access control information; and

distribution logic programmed to distribute the access control information to at least one access device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels, wherein the access device is operable to transmit the channel to the host device and is logically closer to the host device than the apparatus for distributing access control information,

whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

26. (original) The computer program of claim 25, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

27. (original) The computer program of claim 26, wherein the distribution logic is programmed to send the access control information to a predetermined multicast group using the reliable multicast mechanism.

28. (original) The computer program of claim 25, wherein the predetermined push mechanism comprises a policy service.

29. (original) The computer program of claim 28, wherein the policy service comprises a Common Open Policy Service (COPS).

30. (original) The computer program of claim 28, wherein the distribution logic is programmed to send the access control information to the access device in the form of policy information using the policy service.

31. (original) The computer program of claim 25, wherein the predetermined push mechanism comprises a management mechanism.

32. (original) The computer program of claim 31, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

33. (original) The computer program of claim 31, wherein the management mechanism comprises a Command Line Interface (CLI).

34. (original) The computer program of claim 31, wherein the distribution logic is programmed to send the access control information from the distribution device to the access device in the form of management information using the management mechanism.

35. (previously presented) An apparatus for providing receiver access control in an internet television system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the apparatus comprising:

distribution logic operably coupled to receive multicast group access control information from a distribution device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels;

host interface logic operably coupled to receive a request from a host device to join a television channel multicast group; and

access control logic operably coupled to determine whether the host device is authorized to join the television channel multicast group based upon the access control information, wherein the apparatus is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

36. (original) The apparatus of claim 35, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

37. (original) The apparatus of claim 36, wherein the distribution logic is operably coupled to join a predetermined multicast group and receive the access control information from the predetermined multicast group using the reliable multicast mechanism.

38. (original) The apparatus of claim 35, wherein the predetermined push mechanism comprises a policy service.

39. (original) The apparatus of claim 38, wherein the policy service comprises a Common Open Policy Service (COPS).

40. (original) The apparatus of claim 38, wherein the distribution logic is operably coupled to receive the access control information from the distribution device in the form of policy information using the policy service.

^

41. (original) The apparatus of claim 35, wherein the predetermined push mechanism comprises
a management mechanism.

42. (original) The apparatus of claim 41, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

43. (original) The apparatus of claim 41, wherein the management mechanism comprises a Command Line Interface (CLI).

44. (original) The apparatus of claim 41, wherein the distribution logic is operably coupled to receive the access control information from the distribution device in the form of management information using the management mechanism.

45. (previously presented) A computer program embedded in a tangible storage medium for controlling a computer system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the computer program comprising:

distribution logic programmed to receive multicast group access control information from a distribution device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels;

host interface logic programmed to receive a request from a host device to join a television channel multicast group; and

access control logic programmed to determine whether the host device is authorized to join the television channel multicast group based upon the access control information, wherein the host interface logic is executed by a device that is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

46. (original) The computer program of claim 45, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

47. (original) The computer program of claim 46, wherein the distribution logic is programmed to join a predetermined multicast group and receive the access control

information from the predetermined multicast group using the reliable multicast mechanism.

48. (original) The computer program of claim 45, wherein the predetermined push mechanism comprises a policy service.

49. (original) The computer program of claim 48, wherein the policy service comprises a Common Open Policy Service (COPS).

50. (original) The computer program of claim 48, wherein the distribution logic is programmed to receive the access control information from the distribution device in the form of policy information using the policy service.

51. (original) The computer program of claim 45, wherein the predetermined push mechanism comprises a management mechanism.

52. (original) The computer program of claim 51, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

53. (original) The computer program of claim 51, wherein the management mechanism comprises a Command Line Interface (CU).

54. (original) The computer program of claim 51, wherein the distribution logic is programmed to receive the access control information from the distribution device in the form of management information using the management mechanism.

55. (previously presented) An internet television system for delivering a video signal to a host device for display, comprising:

a distribution device in communication with at least one access device over a communication network, wherein the distribution device uses a predetermined push mechanism to distribute multicast group access control information to the at least one access device in order to reduce delay in authentication when a host device changes television channels, and wherein the at least one access device uses the access control information to control access to at least one television channel multicast group, wherein the access device is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

Appendix B - Evidence Submitted

None.

Appendix C - Related Proceedings

None.